USE OF PACKET HASHES TO PREVENT TCP RETRANSMIT OVERWRITE ATTACKS

ABSTRACT OF THE DISCLOSURE

Embodiments of the invention are directed to systems that detect maliciously formed TCP/IP retransmit packets attempting to pass through an intrusion detection system (IDS) and prevent them from reaching their destination by forcing early flow termination. The IDS may be configured to track a hash of certain fields in each packet. This set of hashes is maintained for all of the packets in the currently open TCP window for each flow. If the hash of a retransmit packet does not match the cached hash of the corresponding original packet, the system concludes that there is an attack under way and terminates the flow. The hash function may range in complexity and security from low complexity and relative insecurity to high complexity and high security. Hash algorithms may also be used in conjunction with a private seed value concatenated with the packet fields prior to hashing.